



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/567,209

02/03/2006

Wilhelmus Franciscus Johanne Verhaegh

NL031006

9671

24737

7590

05/22/2008

PHILIPS INTELLECTUAL PROPERTY & STANDARDS

P.O. BOX 3001

BRIARCLIFF MANOR, NY 10510

EXAMINER

JOHNS, CHRISTOPHER C

ART UNIT

PAPER NUMBER

3621

MAIL DATE

DELIVERY MODE

05/22/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/567,209	<b>Applicant(s)</b> VERHAEGH ET AL.	
	<b>Examiner</b> Christopher C. Johns	<b>Art Unit</b> 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 19 February 2008.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Acknowledgements***

1. Amendment of 19 February 2008 has been received.
2. Claims 1, 2, 6, 7, 9, and 11-13 have been amended.
3. Claims 1-13 are pending.

### ***Response to Amendment***

4. Applicants' amendment of 19 February 2008 is sufficient to overcome the Objections to the title and drawings, and the rejections under 35 USC §112 and 35 USC §101.
5. Examiner notes that throughout the Amendment, Applicants have referred to the noted prior art as "Carry". The correct name for the author of the prior art is John Canny. The Examiner has interpreted arguments against "Carry" to be arguments against "Canny".

### ***Claim Rejections - 35 USC § 102***

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1 and 4-13 are rejected under 35 U.S.C. 102(b) as being anticipated by "Collaborative Filtering with Privacy", a paper by John Canny, in the Proceedings of the 2002 IEEE Symposium on Security and Privacy (hereafter "Canny").
8. As per claims 1, 6, and 11-13, Canny discloses:

9. encrypted first data from a first user, and encrypted second data from a second user

(section 3.2 – “each user has data values...each value is a standard El-Gamal encryption...”);

10. a server configured to obtain the encrypted first and second data (Abstract: "our system can be implemented with untrusted servers"), the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second users to each other (Abstract: “we describe an algorithm whereby a community of user can compute a public 'aggregate' of their data that does not expose individual users' data");

11. computation means for performing a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first users respectively (Abstract: “we describe an algorithm whereby a community of user can compute a public 'aggregate' of their data that does not expose individual users' data"), the similarity value providing an indication of a similarity between the first and second data (Abstract: “the aggregate allows personalized recommendations to be computed by members of the community, or by outsiders”; section 2.1, "Given a vector of user preferences  $P$ , the most likely pair  $(x,n)$ ...”).

12. As per claim 4, Canny discloses:

13. computation means to obtain an encrypted inner product between the first data and the second data, or encrypted sums of shares of the first and second data in the similarity value (section 1.2 - “Collaborative filtering using SVD is not new”), and the server is coupled to a public-key decryption server for decrypting the encrypted inner product or the sums of shares

and obtaining the similarity value (section 3.2 – “each value is a standard El-Gamal encryption of the exponentiation”).

14. As per claim 5, Canny discloses:

15. the similarity value is obtained using a Pearson correlation or a Kappa statistic (section 5.3 – “For instance, a Pearson correlation and personality diagnosis use the entire user dataset to generate new recommendations”)

16. As per claim 7, Canny discloses:

17. first or second data comprises a user profile of the first or second user respectively (Abstract – “e-commerce and...direct recommendation applications”), the user profile indicating user preferences of the first or second user to media content items (section 1 – “personalized purchase recommendations [about] restaurants, bars, movies, and interesting sights”).

18. As per claim 8, Canny discloses:

19. first or second data comprises user ratings of respective content items (Abstract – “e-commerce and...direct recommendation applications”; section 1 – “personalized purchase recommendations [about] restaurants, bars, movies, and interesting sights”).

20. As per claim 9, Canny discloses:

21. using the similarity value to obtain a recommendation of a content item for the first or second user (Abstract – “an algorithm whereby a community of users can compute a public

‘aggregate’ of their data that does not expose individual users’ data. The aggregate allows personalized recommendations to be computed by members of the community...”; section 2.1 – “Given a vector of user preferences  $P...$ ”).

- 22. As per claim 10, Canny discloses:
- 23. recommendation is performed using a collaborative filtering technique (See title of the paper, 1<sup>st</sup> sentence of Abstract, and section 1).

### ***Claim Rejections - 35 USC § 103***

- 24. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

- 25. Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Canny, in view of the Paillier cryptosystem.
- 26. As per claim 2, Canny teaches:
- 27. the second user calculates, through computational means, an encrypted inner product between the first data and the second data (section 1.2 – Canny discloses that collaborative filtering through Singular Value Decomposition (SVD) is well-known and "not new"), and provides the encrypted inner product to the first user via the server, the first user decrypting the encrypted inner produce for obtaining the similarity value through computational means (Canny does not explicitly disclose that the SVD of the data is encrypted, since it only mentions that the

usage of SVD for collaborative filtering is non-novel. Canny's goal is to provide for a private system where information cannot be leaked. Paillier teaches a cryptosystem. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt the data in an SVD collaborative filtering system, because of the want to provide for privacy and security of the data. A person having ordinary skill in the art would appreciate the advantage that comes from this – namely, that the data communicated between users would be protected from those who would attempt to steal personal information from it. Decrypting the data would be necessary as is inherent with any encrypted data).

28. As per claim 3, Canny teaches:

29. computation means is realized using a Paillier cryptosystem, or a threshold Paillier cryptosystem using a public key-sharing scheme (Appendix A, page 12, where the system uses “cryptographic homomorphism” for the computation of the vector sums. It does not explicitly mention using a Paillier cryptosystem or a threshold Paillier cryptosystem for the computation. The Paillier cryptosystem, published in EUROCRYPT in 1999, is a homomorphic public-key cryptosystem that is based on composite degree residuosity classes. In the original paper, on page 236, Paillier notes that the system is useful for self-blinding data, and, on page 235, that it possesses additive homomorphic properties (meaning that data can be added to encrypted data without needing to decrypt the original data). The system in Canny does not explicitly use the Paillier cryptosystem for its computations. However, the Paillier system is a cryptosystem that would do exactly what the system in Canny desires – it is a homomorphic cryptosystem that allows for self-blinding. The motivation to use the Paillier system exists because it is perfectly

suited for Canny's needs, and would be a simple substitution for Pedersen's scheme (cf. section 3.1, "After applying Pedersen's protocol..."). Therefore, it would have been obvious to one skilled in the art at the time of the invention to use the Paillier cryptosystem in the system in Canny, because of the interchangeability and the motivating statements in the Paillier publication. A person having ordinary skill in the art would recognize the advantage that comes from using Paillier as a cryptosystem in Canny, namely that the system in Canny would preserve privacy appropriately).

### ***Response to Arguments***

30. Applicant's arguments filed 19 February 2008 have been fully considered but they are not persuasive.

31. Concerning Applicants' main argument (pages 14-15) that Canny does not teach performing a computation between first and second data, because it uses a "public aggregate" matrix to perform its computations, the Examiner notes that section 2 says "Assume there are  $n$  users...". If  $n$  is set to 2, then the system in Canny *is* performing a computation between two users' data, since the public aggregate matrix will contain one of the users' data and the second user will be able to compare his data to this matrix (of one set). This same logic covers the arguments for claims 1, 6, and 11-13.

32. Applicants also aver that "one user's data is never sent in encrypted form to any other user in the [Canny] system". The Abstract in Canny notes that it "can be implemented with untrusted servers, or...a fully peer-to-peer (P2P) system". In a peer-to-peer system, data *is* sent to the other users, as this is the nature of this type of system.



33. Applicants argue on page 16 that “there are many techniques in practice by which authentic public key can be distributed”. The inclusion of the El-Gamal cryptosystem is not meant to refer to the Key Distribution problem in cryptography. Furthermore, the “decryption server” in the instant application is read to mean a system for decrypting data. Nowhere in the claims is it stated that the “public-key decryption server” must be “separate”, as is stated in the arguments.

34. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the arguments on pages 20-22) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

35. Throughout the arguments (pages 16, 18), Applicants state that the Examiner has “[alleged] that the [Canny] reference discloses the ‘gist’” of the present application's claimed invention. The Examiner never used the word “gist”, nor did the Examiner attempt to distill the claimed invention to its primitive parts in order to reject it.

***Conclusion***

36. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure.

37. “Amazon.com Recommendations – Item-to-Item Collaborative Filtering”, appearing in Internet Computing, published by the IEEE Computer Society, January/February 2003.

38. “E-Commerce Recommendation Applications”, a paper appearing in “Data Mining and Knowledge Discovery”, from January 2001.

39. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 C.F.R. §1.136(a).

40. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 C.F.R. §1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

41. Because this application is now final, Applicant(s) are reminded of the USPTO's after final practice as discussed in MPEP §714.12 and §714.13 and that entry of amendments after final is *not* a matter of right. Furthermore, suggestions or examples of claim language provided by the Examiner are just that—suggestions or examples—and do not constitute a formal requirement mandated by the Examiner. Unless stated otherwise by an express indication that a

claim is “allowed,” exemplary claim language provided by the Examiner to overcome a particular rejection or to change claim interpretation has *not been addressed* with respect to other aspects of patentability (*e.g.* §101 patentable subject matter, §112 1<sup>st</sup> paragraph written description and enablement, §112 2<sup>nd</sup> paragraph indefiniteness, and §102 and §103 prior art).

Therefore, any claim amendment submitted under 37 C.F.R. §1.116 that incorporates an Examiner suggestion or example or simply changes claim interpretation will nevertheless require further consideration and/or search and a patentability determination as noted above.

42. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher C. Johns whose telephone number is (571)270-3462.

The examiner can normally be reached on Monday - Friday, 9 am to 5 pm.

43. If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

44. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher C Johns  
Examiner  
Art Unit 3621

CCJ

/ANDREW J. FISCHER/  
Supervisory Patent Examiner, Art Unit 3621